IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | CASE NO.: 1:18-CR-22 |
| | ) | |
| Plaintiff | ) | JUDGE: SOLOMON OLIVER, JR. |
| | ) | |
| vs. | ) | **DEFENDANT PHILLIP DURACHINSKY'S** |
| | ) | **MOTION TO SUPPRESS EVIDENCE** |
| PHILLIP DURACHINSKY, | ) | **AND STATEMENTS** |
| | ) | |
| Defendant | ) | **EVIDENTIARY HEARING REQUESTED** |

Now comes Defendant Phillip Durachinsky, by and through counsel, and respectfully moves this This Honorable Court for an order suppressing evidence, to wit: Defendant's computer and external hard drives, Defendant's work computer and flash drive (derivative evidence), computer data from Defendants' personal and work computers, computer data from Defendant's external hard drives, derivatively resulting statements made by Defendant, as well as any and all other derivatively obtained evidence. All said evidence was obtained by the Government in violation of Defendant's rights under the Fourth Amendment of the United States Constitution. Defendant asserts that his personal computer, and electronic storage device were seized without search warrants, and all additional computer related evidence was "fruit of the poisonous tree". Defendant further asserts that his personal computer was initially searched without a search warrant, and was unlawfully again searched subsequent to its seizure, but prior to the issuance of a search warrant. Eventually, investigators did get search warrants to search Defendant's computers, and they discovered evidence (computer data) that included text files, picture files, and log files, which the Government will seek to introduce at trial. As a derivative result of the illegally obtained evidence, Defendant later made

incriminating statements to investigators. These statements, as well as any and all other derivative evidence, must also be suppressed as "fruit of the poisonous tree".

Defendant adamantly contends that the Government will be unable to show that the search and seizure at issue in this case falls within any recognized exception to the warrant requirement of the Fourth Amendment. Although Defendant obviously does not know what the Government will specifically argue in attempting to justify the warrantless search and seizure, Defendant has tried to anticipate the basic Government arguments in his attached Memorandum in Support.

## MEMORANDUM IN SUPPORT

## STATEMENT OF FACTS

According to discovery provided by the Government, on January 4, 2017, Case Western Reserve University (CWRU) was contacted by a third party regarding network scanning and an infected system on the third party's network. The third party provided CWRU indicators of compromise, i.e., computer forensic artifacts indicating a computer infection, which were used in the malware communications found on the third party system. The third party stated that it believed that because of the communication between the third party's infected computer and the CWRU system, the CWRU system was also likely compromised. On January 5, 2017, CWRU contacted the FBI related to the notification from the third party, and confirmed that an intrusion had occurred on the CWRU network. CWRU identified over 100 computers at CWRU with active Internet connections as being infected with the malware. On January 6, 2017, the FBI interviewed CWRU Information Technology (IT) security personnel and imaged an

infected computer. The FBI's review of the image confirmed that computers at CWRU had been compromised for several years. CWRU determined that an IP address, associated with the malware that had infected the CWRU computers, had also been used to access the alumni email account of CWRU alumnus Defendant Phillip Durachinsky. Presumably, on or about January 6, 2017, Defendant became the primary suspect in the computer malware attack on the CWRU computers. On January 10, 2017 the FBI continued with its full investigation into the matter including the performing of criminal history and bureau of motor vehicle checks on Defendant. Base on those records searches the FBI learned of Defendant's home address located in North Royalton, Ohio.

On January 18, 2017, at approximately 10:00 pm, five FBI agents, and two North Royalton police officers went to Defendant's home, where he lived with his parents, to conduct what is referred to in the FBI 302 report as a "knock and talk". At the time, Defendant was not at home, but rather was at his job in Cleveland. Neither the FBI or North Royalton had a search warrant or arrest warrant, nor had either agency apparently ever sought warrants prior to going to Defendant's home. Apparently, the law enforcement agents did not believe that they had adequate probable cause, at that time, in order to obtain a search warrant for Defendant's home or for his computer. Defendant's sixty-one year old father, Phillip Durachinsky (Mr. Durachinsky) answered the door. When Mr. Durachinsky opened the door, he was greeted by two FBI agents. After being advised as to the identity of the agents, Defendant's father agreed to talk, and let those two agents in the agents in the residence (the other three agents who ultimately entered the home were never invited inside, but entered without the

Durachinskys' invitation or consent). Also present at the residence was Mr. Durachinsky's sixty year old wife Marylou Durachinsky (Mrs. Durachinsky), who was dressed in her nightgown, and had been in bed at the time law enforcement officers came to the home. At one point, a third FBI agent opened the front door and entered the house while Mr. Durachinsky was speaking with the first two agents at the dining room table. Mrs. Durachinsky indicated their son also lives at the residence but was at work. Mr. and Mrs. Durachinsky were advised that the FBI was conducting an investigation involving suspicious network activity originating from an IP address registered to their home. Mr. Durachinsky led the agents to the basement where his desktop computer was located. Mr. Durachinsky signed a "Consent to Search Computer(s)" form for his HP desktop computer with serial number 4CE4100VNB located in the basement. While Mr. Durachinsky was in the basement, two more FBI agents let themselves in through the front door. There were now five FBI agents in the relatively small home. Mrs. Durachinsky showed a laptop in the living room that she uses. Mrs. Durachinsky signed "Consent to Search Computer(s)" form for the Dell laptop with tag 3JR2402 located in the living.

Mrs. Durachinsky was then asked if there were any other computers in the house. She indicated that Defendant had a laptop in his room that he remotes into from work (this room is a separate room from Defendant's bedroom, and is located adjacent to Defendant's bedroom down a hallway). The FBI agents indicated that they wanted to look at the Defendant's computer. Mrs. Durachinsky told the FBI agents that they should call him at work first, and she did not give the FBI agents permission to look at Defendant's computer. The FBI called Defendant at his job, and Defendant wanted to

know whether they had a warrant. The FBI agent speaking with Defendant told Defendant that they can seize and seal it, and then get a warrant. Defendant expressly indicated that he did not consent to the seizure of his computer, and he told them that they could not take his computer without a search warrant. Further, Defendant did not give his consent for FBI agents to open the computer lid and look at any contents on the computer screen, input any information into his computer, or use his computer in any manner. Defendant indicated that he was leaving work, and coming directly home with some friends from work.

Mr. and Mrs. Durachinsky then went down the hallway and showed the FBI agents Defendant's computer room, which was his childhood bedroom, was used exclusively by Defendant, and which contained his laptop computer. Mr. and Mrs. Durachinsky opened the door, and pointed to an ACER Aspire laptop sitting on a desk. Although one of the FBI agents in the 302 report indicated that he noticed the laptop lid was "slightly open" and observed the mouse pointer was moving and the screen was updating, Defendant strongly asserts that he had shut the laptop lid when he was last finished using the computer, and that he would never have left the laptop lid partially open. Defendant maintains that he always keeps the laptop lid closed. Additionally, Defendant contends that a desk chair, which was positioned such that it would have blocked any view of a possible open computer screen, would have had to have been moved by the FBI agents prior to them having been able to view the computer screen, even assuming arguendo, that the laptop lid was slightly open. At no time did either Mr. or Mrs. Durachinsky give permission to the FBI agents to enter or search Defendant's computer room. Regardless, FBI agents entered the room, and soon after, the laptop

lid was opened. One of the FBI agents believed someone may have been remotely accessing the laptop. At that point in time, another of the FBI agents unplugged the power cord from the router located in the basement in order to prevent the remotely connected user from deleting information from the laptop. FBI agents also took cell phone video and still shots of the laptop screen. One of the FBI agents entered commands on the ACER laptop to determine if there was encryption on the laptop. No encryption was observed in use on the laptop by the agent. The laptop belonging to Defendant, described as an ACER Aspire laptop and a Western Digital external hard disk drive, which was located next to the laptop but disconnected from the laptop, was seized by the FBI agents.

When Defendant arrived at his home, it was once again made clear to the FBI agents that Defendant did not consent to either the search or seizure of his computer. The agents responded that they were seizing the computer due to exigent circumstances, and a search warrant would be applied for later that night (it was issued in the early morning of the following day). Searches were not conducted of the HP desktop and Dell laptop computers belonging to Mr. and Mrs. Durachinsky, at that time.

On a subsequent date, the FBI went to Defendant's work place and spoke with Defendant's employer. The FBI requested consent from the employer to search Defendant's work computer (Lenovo S41-70) as well as an attached USB drive (SanDisk Cruzer Glide 128 GB). Apparently, the FBI agents did not have a search warrant at that time for the computer or USB drive. The FBI did eventually obtain a search warrant for those items, based in large part on the evidence uncovered during the search of Defendant's personal laptop computer. Although Defendant's employer

signed a written consent form authorizing the seizure and search of Defendant's work computer, Defendant never consented to either the seizure or the search of those items.

Based upon a review of the logs of Defendant's computer, the following timetable for Wednesday January 18, 2017, regarding the FBI agents' actual physical contact with Defendant's computer, will be shown as follows:

- 10:05:27 am - Defendant closes the lid of his lap top computer prior to leaving for work.
- 10:13:52 pm – FBI agents open lap top lid of computer.
- 10:14:00 pm – Voicemail to Defendant's boss, Mark Lorkowski. (approx. time)
- 10:14:56 pm – FBI agents begin videotaping (Video #1) of lap top computer screen.
- 10:15:31 pm – End of recording Video #1.
- 10:15:43 pm - FBI agents begin videotaping (Video #2) of lap top computer screen.
- 10:16:03 pm - End of recording Video #2.
- 10:16:16 pm – FBI agents take photo #1 of lap top computer screen.
- 10:17:15 pm – FBI agents disconnect Internet.
- 10:18:38 pm – FBI agents use lap top touchpad for the first time.
- 10:32:29 pm - FBI agents take photo #2 of lap top computer screen.
- *10:40:42 pm - /home/me2/.bash history modified by FBI agents.*
- 10:42:37 pm - FBI agents begin videotaping (Video #3) of lap top computer screen.
- 10:42:39 pm - End of recording Video #3.
- 10:42:46 pm - FBI agents begin videotaping (Video #4) of lap top computer screen.
- 10:45:18 pm - End of recording Video #4.
- 10:46:43 pm - FBI agents close lap top lid of computer.
- 10:46:45 pm – FBI agents unplug power cable (battery discharging).

- *10:50:19 pm – FBI agents re-open laptop lid of computer*
- 10:52:47 pm – FBI agents reconnect household Internet.
- 10:55:00 pm – FBI agents take laptop computer out of the house. (approx. time)
- 11:05:00 pm – FBI agents (all) leave the house. (approx. time)
- 11:50:19 pm – FBI agents plug in laptop power cable (battery charging).
- 11:50:19 pm – FBI agent's re-open laptop lid.
- 11:52:08 pm – FBI agents begin using touchpad.
- 12:10 am to 1:08 am (January 19, 2017) - FBI agents were accessing and running commands on the laptop computer, *including extra filesystem mounted by user me2 at 12:10:55 am and tmp1.filesystem mounted by user me2. At 12:11:01 am.*
- 4:40 am (January 19, 2019) – FBI agents obtain signed search warrant for laptop computer.

As the above laptop computer logs themselves will show, prior to obtaining a search warrant, FBI agents repeatedly opened the laptop lid, ran commands on Defendant's computer, and accessed computer data on Defendant's computer. These activities were undertaken by the FBI agents despite being expressly notified by Defendant that they did not have his consent to do so.

In preparation of this motion to suppress, Defendant, through counsel, retained the services of a forensic computer expert, C. Matthew Curtin. A copy of his expert report relevant to this suppression motion is attached to this motion, and is hereby incorporated into this motion, along with a copy of Mr. Curtin's curriculum vitae. **(See Attached Exhibit A)**.

Of specific importance, to the issues at bar, is the following determination made by Mr. Curtin:

> "We find that evidence shows that the condition in which law enforcement officials discovered the Acer Laptop was with the screen blanked and the lid open no more than 1 and 3/4 inches. No onscreen activity would be visible before physical manipulation of the lid to open it further, which happened at 22:13 local time according to the computer's clock."

Defendant asserts that Mr. Curtin's forensic review and conclusions, as set forth in his expert report, entirely corroborate the Defendants' position regarding the factual circumstances surrounding the Government's warrantless searches and seizure of Defendant's lap top computer on January 18, 2019 through January 19, 2019.

## LAW AND ARGUMENT

### I. Defendant's Standing

An individual has standing to challenge a search or seizure based upon a Fourth Amendment violation when that individual has an objectively reasonable expectation of privacy in the item that was seized and searched. Katz v. United States, 265 U.S. 57 (1967); United States v. Gillis, 358 F.3d 386, 391 (6th Cir. 2004). "[S]tanding to challenge the search of [a place] hinges on whether he had a reasonable expectation of privacy in the [place]. To establish such an expectation, the defendant must show (1) that he had a subjective expectation of privacy, and (2) that his expectation was objectively reasonable." United States v. Washington, 573 F.3d 279,283 (6th Cir. 2009).

In the case at bar, the laptop computer which was searched and then seized from Defendant's computer room at his home, as well as the external hard drive located next to the laptop computer were Defendant's property. The room that was searched in

Defendant's home was his computer room. As such, Defendant clearly had an objective reasonable expectation of privacy in both the computer and external hard drive, as well as his computer room located in his house. Thus, he has standing to challenge the search and seizure of both items.

## II. The Search And Seizure Without A Warrant Was Unreasonable Under The Fourth Amendment

As the United States Supreme Court stated in Katz v. United States, 389 U.S. 347 (1967):

> Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," Agnello v. United States, 269 U. S. 20, 269 U. S. 33, for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police. . . ." Wong Sun v. United States, 371 U. S. 471, 371 U. S. 481-482. "Over and again, this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes," United States v. Jeffers, 342 U. S. 48, 342 U. S. 51, and **that *searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment -- subject only to a few specifically established and well delineated exceptions.***
>
> **(emphasis added)**

Therefore, since the searches at issue in this case – Defendant's home, Defendant's computer room, Defendant's computer and external hard drive, and the seizure of the computer and external hard drive were done without a warrant, they were per se Constitutionally unreasonable, and any evidence obtained as a result of these Government actions must be suppressed.

The exceptions, mentioned in Katz, supra, relevant to the case at bar, include (1) "exigent circumstances" - when probable cause to search or seize exists and officers

reasonably believe that contraband or evidence may be destroyed or removed before a search warrant could be obtained. See Mincey v. Arizona, 437 U.S. 385 (1978); (2) the individual "consents". See Illinois v. Rodriguez, 497 U.S. 177, 183-84, (1990); (3) the item to be seized is an instrumentality of the crime within "plain view", requiring the officer to be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent. *See* Horton v. California, 496 U.S.128, 136 (1990). None of these exceptions are available to the Government in the case at bar.

## III. The Government Cannot Show Exigent Circumstances

Circumstances that qualify as "exigent" lie in one of four categories: (1) hot pursuit of a fleeing felon; (2) imminent destruction of evidence; (3) the need to prevent a suspect's escape; and (4) a risk of danger to the police or others. United States v. Johnson, 22 F.3d 674, 680 (6th 1994). The burden of proof is on the government to prove the exigency, and as the Sixth circuit noted in United States v. Purcell, "Qualification for this exception is not easy." 526 F.3d 953 (6th 2008). The Government cannot prove any of the four exceptions to the search warrant requirement to justify the FBI agents' warrantless search and seizure of Defendant's laptop computer and external hard drive. Clearly, the officers were not in hot pursuit of someone carrying the computer, there was no risk of danger to the agents or others, nor was seizure of the computer necessary to prevent a suspect's escape or to mitigate a risk of danger to the agents or to others. Lastly, the Government will be able to present nothing to support a claim that the seizure of the computer was necessary to prevent the destruction of evidence. See Mincey v.

Arizona, 437 U.S. 385, 394 (1978) (exigent circumstances do not justify search or seizure where police guard at door could prevent loss of evidence). United States v. Jeffers, 342 U.S. 48, 52 (1951) (same); Flippo v. West Virginia, 528 U.S. 11 (1999)(no "crime scene" exception exists for getting a warrant); cf. U.S. v. Beasley, 199 Fed.Appx. 418 (6th 2006) (where officers, even upon seeing baggies of marijuana and scales during a protective sweep, secured the motel room and procured a warrant).

The principles governing warrantless searches based on "exigent circumstances" are fairly well settled. In the Fourth Amendment, the Founders required a warrant for searches and seizures because they did not trust constables, sheriffs and other officers to decide for themselves when they had probable cause to search houses, individuals and places of business. The first and most important principle is that searches must ordinarily be cleared in advance as a part of the judicial process. In Coolidge v. New Hampshire, 403 U.S. 443, 454-55, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971) (footnotes omitted), the Supreme Court explained: Thus the most basic constitutional rule in this area is that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment--subject only to a few specifically established and well-delineated exceptions." The exceptions are "jealously and carefully drawn," and there must be "a showing by those who seek exemption ...that the exigencies of the situation *made that course imperative."* "[T]he burden is on those seeking the exemption to show the need for it." (Emphasis added and footnotes omitted.) In order for a warrantless search to pass muster, probable cause must exist, but "no amount of probable cause can justify a warrantless seizure," *id.* at 471, 91 S.Ct. 2022, because, in addition, the cause of the search must be based on an "emergency" and

hence, "inadvertent" or unanticipated. "Where the discovery is anticipated, where the police know in advance the location of the evidence and intend to seize it, the situation is altogether different." *Id.* at 470, 91 S.Ct. 2022.

Here, even if the warrantless entry into the Defendant's residence was justified by the consent of Defendant's parents, the search, seizure and removal of the computer from his home was not. As an initial matter, the seizure of the computer was not supported by probable cause, which is itself violative of the Fourth Amendment. See Arizona v. Hicks, 480 U.S. 321, 325 (1987). However, even if the officers had probable cause—and not merely a hunch that the computer contained evidence of computer crimes—that alone does not give the officers license to seize the computer and remove it from Defendant's residence. Absent one of the aforementioned exceptions, the Fourth Amendment still requires that the officers secure a warrant to seize property.

If the FBI agents indeed had probable cause to support their contention that the computer contained contraband or evidence, the Fourth Amendment dictates that they should have secured a warrant authorizing them to seize the property. They failed to do so and, instead, seized the property without a warrant and without any justification for an exception to the warrant requirement. Consequently, the evidence must be suppressed as having been procured in violation of Defendant's Fourth Amendment rights.

Accordingly, the seizure of the computer violated the Fourth Amendment and all evidence seized as a result of the seizure must be suppressed as "fruits of the poisonous tree." See Wong Sun v. United States, 371 U.S. 471, 485 (1963).

## IV. No Voluntary Consent To Search House

"Whether consent is voluntary is a question of fact determined from the totality of the circumstances." United States v. Lopez-Medina, 461 F.3d 724, 737 (6th Cir. 2006). The Government has the burden to prove " through clear and positive testimony that the consent to search was given voluntarily. Consent is voluntary when it is unequivocal, specific and intelligently given, uncontaminated by any duress or coercion." United States v. Ivy, 165 F.3d 397, 402 (6th Cir. 1998) (internal quotation marks and citations omitted). This determination is based on the totality of the circumstances, and this Court has identified a number of factors that are often relevant to this consideration including the age, intelligence, and education of the individual giving consent, whether the individual understands that he or she has a right to refuse consent, whether the individual understands his or her constitutional rights, the length and nature of any detention, and to what extent the police engaged in coercive or punishing conduct. See, e.g., United States v. Elkins, 300 F.3d 638, 647 (6th Cir. 2002). Part of this Court's voluntariness analysis is a consideration of "the circumstances surrounding the search for 'more subtle forms of coercion that might flaw [an individual's] judgment." United States v. Moon, 513 F.3d 527, 537 (6th Cir. 2008) (alteration in original) (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 227, 93 S.Ct. 2041, 36 L.Ed.2d 854 (1973)).

In U.S. v. Tatman 397 Fed.Appx. 152 (6th Cir. 2010) the Court held that a "consent search" of the Defendant's home, based on a written consent form, signed by the Defendant's estranged wife, was not voluntary. The Court went on to state the applicable law as follows:

> " Whether consent is voluntary is a question of fact determined from the totality of the circumstances." United States v. Lopez-Medina, 461 F.3d 724, 737 (6th Cir.

> 2006). ……. The Government has the burden to prove " through clear and positive testimony that the consent to search was given voluntarily. Consent is voluntary when it is unequivocal, specific and intelligently given, uncontaminated by any duress or coercion." United States v. Ivy, 165 F.3d 397, 402 (6th Cir. 1998) (internal quotation marks and citations omitted). This determination is based on the totality of the circumstances, and this Court has identified a number of factors that are often relevant to this consideration including the age, intelligence, and education of the individual giving consent, whether the individual understands that he or she has a right to refuse consent, whether the individual understands his or her constitutional rights, the length and nature of any detention, and to what extent the police engaged in coercive or punishing conduct. *See, e.g.*, United States v. Elkins, 300 F.3d 638, 647 (6th Cir. 2002). Part of this Court's voluntariness analysis is a consideration of "the circumstances surrounding the search for 'more subtle forms of coercion that might flaw [an individual's] judgment." United States v. Moon, 513 F.3d 527, 537 (6th Cir. 2008) (alteration in original) (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 227, 93 S.Ct. 2041, 36 L.Ed.2d 854 (1973)).

In the case at bar, as in Tatman, there were a number of subtle, and not so subtle forms of coercion that operated upon Defendant's parents in such a manner so as to make their consent for law enforcement agents to enter the house, and go to particular parts of the home, specifically the hallway outside Defendant's computer room, not voluntary. The presence of seven law enforcement agents appearing at the door of a naïve, older, law-abiding couple, late at night (10:00 pm), in the middle of winter, stating that they were investigating a serious crime is at best intimidating, and at worst, outright coercive. The fact that the lead investigators identified themselves as FBI agents certainly served as another subtle form of coercion for Defendant's parents to allow the agents into the house, show them their respective computers, and take them through various parts of the home. Moreover, there is no indication that a complete explanation of their rights and options, regarding "cooperating" with the FBI agents' investigation, was given to either Mr. or Mrs. Durachinsky.

Defendant asserts that based upon the totality of the circumstances, the Government will not be able to meet its burden in proving that Mr. and Mrs. Durachinsky's consent for the law enforcement agents to enter and wander about Defendant's home was voluntary.

## V. No Consent To Search Computer Room Or Search And Seize Personal Computer

It is expected that the Government will assert that Defendant's parents gave the law enforcement officers consent to enter the their and the Defendant's house, consent to be in the rooms in which Mr. and Mrs. Durachinsky led agents into in order to show them their respective computers, and consent to be in the hallway outside of Defendant's computer room. However details of Mr. and Mrs. Durachinsky's alleged consent to search, and scope thereof, are unclear. The Government bears the burden of proving the alleged consent to search was voluntary. United States v. Erwin, 155 F.3d 818, 823 (6th Cir. 1998). An evidentiary hearing is thus necessary to determine the circumstances of the alleged grant of consent by Mr. and Mrs. Durachinsky and, if consent was granted, to determine whether the search exceeded the scope of any such consent. A person who consents to a warrantless search has the right to restrict the scope of the search. Florida v. Jimeno, 500 U.S. 248, 252, (1991); U.S. v. Tatman, 397 Fed.Appx. 152 (6th Cir. 2010). Based upon FBI reports, statements made by Mr. and Mrs. Durachinsky, as well as the Defendant's version as to what occurred relevant to the search and seizure of his computer, it seems undisputed that Mr. and Mrs. Durachinsky, and Defendant, all expressly denied consent for the agents to either search or seize his computer. It also appears that the Government will not be able to

show that any consent to enter various parts of their home, given by the Durachinskys, extended to Defendant's computer room. If the Government cannot show that agents had consent to enter Defendant's computer room, it would have been physically impossible for them to have seen the computer screen (even assuming arguendo that their account of the computer lap top lid being "slightly open" is correct). If they could not see the computer screen, they would not have been able to see someone possibly remotely accessing the computer, and would not have learned the additional factual circumstances that led them to reach the probable cause threshold that they were lacking when they initially went to Defendant's house. It would also fatally undercut the Government's argument that agents were justified in further searching and accessing the computer base on "exigent circumstances".

## VI. The Data On The Laptop Screen Was Not In Plain View

It is expected that the Government will argue that it was the agents' viewing of the contents of the laptop computer screen, and the visible remote accessing of that screen that helped furnish the probable cause, necessary to justify the further search of the computer and the seizure as well, under the theory that exigent circumstances then existed. Evidence of a crime may be seized without a warrant under the "plain view" exception to the warrant requirement. To rely on this exception, the agent must be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent. See Horton v. California, 496 U.S. 128, 136 (1990). A warrantless seizure of property is justified under the "plain view" exception when the incriminating nature of the object or thing to be seized is "immediately apparent." Texas

v. Brown, 460 U.S. 730 (1983); United States v. McLernon, 746 F.2d 1098 (6th Cir. 1984).

In Arizona v. Hicks, 480 U.S. 321 (1987), a case on point with the case at bar, a bullet fired through the floor of the defendant's apartment, injuring a man on the floor below. The police entered the defendant's apartment to search for the shooter and additional victims. Id. While conducting a protective sweep of the apartment, the police noticed expensive stereo equipment that they suspected was stolen. Id. They moved the equipment in order to read and record the serial numbers. Id. After running the serial numbers through their data base and learning that the equipment had been taken during an armed robbery, the police immediately seized the equipment. Id. The Supreme Court held that the police officer's action in merely moving the equipment in order to record the serial number violated the Fourth Amendment. Id. at 323. The Supreme Court explained that because the officers had only "reasonable suspicion"—less than probable cause—to believe that the equipment was stolen, the government could not rely on the plain view doctrine as it applies to seizures. Id. at 322. If the officers had had probable cause to believe that the equipment had been stolen, the Court stated that the plain view doctrine would have sustained the seizure of the equipment without a warrant. Id. In the absence of probable cause, the Supreme Court affirmed the lower court's decision to suppress the evidence seized from the defendant's apartment. Id. at 321.

There was nothing about the presence of a laptop computer, located in a person's (Defendant's) computer room that was out of the ordinary or suspicious. Further, since the lid of the laptop was closed, there was absolutely no indication, to any

nearby observer, that the computer was either stolen, contraband, or being used in the commission of a crime. In U.S. v. MacLevain 310 F.3d 434 (6th Cir. 2002), a case involving the seizure of "plain view" evidence, during the execution of a search warrant, the Court suppressed the evidence, and gave a very complete explanation of the "plain view's" concept of "immediately apparent":

> This Court has long deliberated what "immediately apparent" means. We summarized the factors used in many of our prior cases in United States v. Beat, 810 F.2d 574, 576-577 (6th Cir. 1987). We found that while none of these factors is necessary, they are instructive as to what this court has used to find that the criminality of a piece of evidence was "immediately apparent." Id. The factors include l)"a nexus between the seized object and the items particularized in the search warrant," 2)"whether the 'intrinsic nature' or appearance of the seized object gives probable cause to believe that it is associated with criminal activity," and 3) whether "the executing officers can at the time of discovery of the object on the facts then available to them determine probable cause of the object's incriminating nature." Id. (internal citations omitted) (emphasis in original). These factors offer a context within which to evaluate the search and seizure of the four items in McLevain's house……
>
> We begin with the first of the Beat factors. No nexus between the object seized and the items in the search warrant exists in our case. Cauley was the subject of the search. McLevain was an afterthought that has never been explained. The warrant had nothing to do with drug paraphernalia.
>
> The second factor is whether the "intrinsic nature" of the items gives probable cause to believe it is contraband, such as marijuana or cocaine on a table in plain view. The case of Arizona v. Hicks, 480 U.S. 321, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987), is instructive. In that case, the police entered an apartment to search for a shooter. While they were there, an officer saw stereo equipment that he thought was incongruous in the otherwise poorly furnished apartment. Id. at 323, 107 S.Ct. 1149. The officer suspected the stereo was stolen, so he moved the equipment in order to read the serial numbers. Id. The Supreme Court found that "taking action, unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents, did produce a new invasion of respondent's privacy unjustified by the exigent circumstance that validated the entry." Id. at 325, 107 S.Ct. 1149. There was nothing about the "intrinsic nature" of the stereo equipment that proclaimed it as contraband.

McLevain claims that there is nothing about the intrinsic nature of a twist tie, a cigarette filter, a spoon with residue, or a bottle that makes it immediately apparent that those items are contraband. In McLernon, a room was searched pursuant to a cocaine conspiracy, and agents seized a note pad and calendar from a desk, under the "plain view" exception. 746 F.2d at 1104. We said, in that case, these items "were hardly 'intrinsically' incriminating. Indeed such items are found in plain view of virtually every desk across this country. We do not, and cannot, subscribe to a rule of law which allows officers of the state to seize an item as evidence merely because it is in 'plain view.' " Id. at 1125 (emphasis in original). We found that the agents could not have immediately perceived those items as incriminating; "the agents' 'immediate' perceptions produced only visual images of two 'intrinsically innocent' items." Id. Similarly, the items found in McLevain's home might be found under beds, in sinks, and on mantels in many homes, and not exclusively those where methamphetamine is being used. While the cut cigarette filter and the prescription bottle with fluid in it might be out of the ordinary, the police are not authorized to seize odd items. We do not care what the explanation is for the items, but we care that there may be some other explanation for the items. Defense counsel pointed out at oral argument that sometimes smokers who do not want filters in their cigarettes remove them. The "plain view" exception authorizes seizure of only those items that "immediately app[ear]" to be contraband.

In one sense, the facts of this case are similar to those of Texas v. Brown. In that case, an officer made a "plain view" seizure of narcotics at a routine driver's license checkpoint. Id. at 730, 103 S.Ct. 1535. In asking for the driver's license, the officer saw an opaque party balloon, tied at the end, drop from Brown's hand. Id. The officer knew from his experiences in previous narcotics arrests and from conversations with other officers that balloons tied as Brown's was were often used to carry narcotics. Id. at 742-743, 103 S.Ct. 1535. In this case, Detective Acquisito also testified that from his experiences as a narcotics officer he suspected that the twist tie, cigarette filter, spoon, and prescription bottle with liquid were being used with methamphetamine. In both cases, it was the officers's experiences as law enforcement agents that led them to believe that the seemingly quotidian objects were actually drug paraphernalia. The connection between these items and illegal activities, however, is not enough to render these items intrinsically incriminating. The connection is not enough to make their intrinsic nature such that their mere appearance gives rise to an association with criminal activity.

> The final Beal factor examines whether "the executing officers can at the time [3] of discovery of the object on the facts then available to them determine probable cause of the object's incriminating nature." 810 F.2d at 577 (emphasis in original). In United States v. Szymkowiak, 727 F.2d 95, 95 (6th Cir. 1984), the United States had a warrant to search Szymkowiak's home for a television set and some jewelry, and the officers executing the warrant found and seized two guns. The officers thought that the guns had been illegally adjusted to rapidly fire. Id. The officers had to call an agent from the Bureau of Alcohol, Tobacco and Firearms to determine whether the guns were illegal. Id. at 96. We said, "From the facts available to the executing officers in the case before us, they could not determine whether they had discovered evidence of a criminal nature." Id. at 99. Similarly, from the facts available to the officers in McLevain's home, at the time of discovery, they could not determine if they had seen evidence of criminal activity.

"When an item appears suspicious to an officer but further investigation is required to establish probable cause as to its association with criminal activity, the item is not immediately incriminating." United States v. Byrd, 211 F.3d 1270, 2000 WL 491511, **3 (6th Cir. 2000) (unpublished opinion).

There was absolutely nothing about Defendant's laptop computer, sitting on a desk, with its lid closed, that gave rise to probable cause that it was involved in any criminal activity. Therefore, there were no lawful grounds for searching or seizing it. And as emphasized previously, if prior to going to the Durachinskys' home that night, law enforcement agents had adequate probable cause to believe that that a computer belonging to Defendant was involved in criminal activity, the agents would have certainly obtained a search warrant for Defendant's home and his computer. They did not get a warrant because they did not have probable cause. There was nothing observable about Defendant's computer that night which added anything to the law

enforcement agents' probable cause determination. Therefore its search and seizure was unlawful.

## VII. Exigent Circumstances Exception Unavailable To The Government

Pursuant to the United States Supreme Court's holding in Kentucky v. King, 563 U.S. 452 (2011), "The exigent circumstances rule applies when the police do not create the exigency by engaging or threatening to engage in conduct that violates the Fourth Amendment." The Court went on to further state:

> The proper test follows from the principle that permits warrantless searches: warrantless searches are allowed when the circumstances make it reasonable, within the meaning of the Fourth Amendment, to dispense with the warrant requirement. Thus, a warrantless entry based on exigent circumstances is reasonable when the police did not create the exigency by engaging or threatening to engage in conduct violating the Fourth Amendment. A similar approach has been taken in other cases involving warrantless searches. For example, officers may seize evidence in plain view if they have not violated the Fourth Amendment in arriving at the spot from which the observation of the evidence is made, see Horton v. California, 496 U. S. 128, 136–140; and they may seek consent-based encounters if they are lawfully present in the place where the consensual encounter occurs, see INS v. Delgado, 466 U. S. 210, 217, n. 5. Pp. 8–10.
>
> (emphasis added)

In the case at bar, Defendant asserts that in order to view the laptop computer screen, that Government agents violated the Fourth Amendment in multiple ways, including but not limited to: (1) entering Defendant's computer room without consent, and moving a chair that was blocking the view of the laptop computer, and (2) opening the closed lid of the computer and looking at the screen; all done without Defendant's or his parents' consent. Therefore, the "exigent circumstances" exception to the warrant requirement is not available in this case.

## VIII. The Exclusionary Rule Bars The Use Of Evidence And Derivative Evidence Against Defendant

The exclusionary rule bars, from trial, evidence obtained either during or as a direct result of an unlawful invasion of an individual's Fourth Amendment rights. Wong Sun v. United States, 371 U.S. 471, 485 (1963). The exclusionary rule is the only effective tool to ensure the fundamental constitutional guarantee of the sanctity of the home. Id. The policy rationale behind the exclusionary rule is to deter police officers from lawless conduct. In the case at bar, it is clear that the Government agents violated Defendant's Fourth Amendment rights with the search of his home, the search of his computer room, the search of his laptop computer, the seizure of his computer, and the additional searches of his computer prior to the issuance of a search warrant for the search of his computer.

The Government will likely argue that the Court should apply either of the two exceptions to the exclusionary rule in this case, namely, the inevitable discovery doctrine, and/or the independent source doctrine. However, neither doctrine is applicable on the facts of this case.

The independent source doctrine applies to evidence "initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality." Murray v. Williams, 487 U.S. 533 (1988). The Court in United States v. Leake, 95 F.3d 409, 412 (6th Cir. 1996) explained as follows:

> Under the independent source doctrine, evidence will be admitted if the government can show it was discovered through sources "wholly independent of any constitutional violation." Nix, 467 U.S. at 442-43, 104 S.Ct. at 2508-09 (1984). The doctrine ensures that the government is not penalized for wrongdoing when such wrongdoing would not bear on the outcome of the case. "In the classic independent source situation, information which is received through an illegal source is considered to be cleanly

obtained when it arrives through an independent source unrelated to and independent of the unconstitutional search." Murray v. United States, 487 U.S. at 538-39, 108 S.Ct. at 2534 (quotation and citation omitted).

Here, the police seized Defendant's computer, and the evidence contained therein, in one way only—through the warrantless seizure of the computer, after executing an initial warrantless search of the computer. The Government cannot in good faith argue that there is no causal connection between the seizure and initial search of the computer, and the resulting search warrant for that warrant. Clearly, the search warrant affidavit for Defendant's computer and external hard drive incorporated affiant observations that were based on the earlier unlawful searches and seizure. **(See Attached Exhibit B)**. The search warrant affidavit itself contains what the Government contends is probable cause in Paragraphs 20-27 of Exhibit B; said probable cause obtained from the prior unlawful searches and seizure. The doctrine applies only to evidence that was discovered "by means wholly independent of any constitutional violation". Since the additional probable cause was developed only by the unlawful conduct by the Government agents at Defendant's home, and then when the computer was in the custody of the agents (but prior to the issuance of the search warrant), the application of the independent source doctrine would be improper.

The inevitable discovery doctrine, an extrapolation of the independent source doctrine, applies to tainted evidence that would have been obtained inevitably. United States v. Howard, 621 F.3d 433, 451 (6th Cir. 2010). The prosecution must establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means. See Nix v. Williams, 467 U.S. 431, (1984). A successful inevitable discovery argument, "requires the government to proffer clear

evidence 'of an independent, untainted investigation that inevitably would have uncovered the same evidence' as that discovered" as a result of the illegal seizure. United States v. Dice, 200 F.3d 978, 986 (6th Cir. 2000); United States v. Kennedy, 61 F.3d 494, 500 (6th Cir. 1995) (inevitable discovery applied where defendant's illegally searched luggage would have inevitably been found by airline personnel to contain narcotics because of the airline's policy of opening lost luggage).

The inevitable discovery doctrine is conceptually more problematic than the independent source doctrine because it involves a degree of deducing what would have happened rather than simply evaluating what actually happened. Here, the Government may contend that the data on Defendant's computer would have inevitably been discovered had the officers secured the scene, and then obtained a search warrant prior to searching the computer and seizing it. However, even if the Government could somehow prove what is actually mere speculation, it is of no moment because the Sixth Circuit has emphatically rejected the Government's reliance on the inevitable discovery doctrine under the circumstances presented here. In United States v. Haddix, 239 F.3d 766, 768 (6th Cir. 2001), the Court attacked the Government's theory—that it could have obtained a warrant, but chose not to, as follows:

> "Under such a theory, evidence that would constitute probable cause for a warrant, even when that evidence's existence is unknown to the police, is inherently destined to be 'inevitably discovered.'" The court then emphasized, "Let it be absolutely clear: this is untenable. As we have noted before, this position of the United States would 'completely obviate the warrant requirement' and would constitute a 'radical departure from the Fourth Amendment warrant requirement precedent." Id. (quoting United States v. Johnson, 22 F.3d 674, 683-84 (6th Cir. 1990)).

See also, United States v. Quinney, 583 F.3d 891 (6th Cir. 2009) (printer seized from the defendant's residence without a warrant was not admissible under the inevitable discovery doctrine even through the police had probable cause and could have obtained a search warrant); United States v. Bowden, 240 Fed.Appx. 56, 63 (6th Cir. 2007) ("Doubtless, the inevitable discovery doctrine does not permit police, who have probable cause to believe a home contains contraband, to enter a home illegally, conduct a warrantless search and escape the exclusionary rule on the ground that 'the police could have obtained a warrant yet chose not to do so'").

In the present case, application of either the independent source or the inevitable discovery doctrines would sanction "post-hoc rationalization through which the Fourth Amendment's prohibition against illegal searches and seizures can be nullified." United States v. Gross, 624 F.3d 309, 321 (6th Cir. 2010). The exclusionary rule application is particularly important here, where officers have decided to create their own exceptions to the Fourth Amendment's requirement—where officers choose expediency or, perhaps, budget concerns, over a citizen's right "to be secure in [his] person, house, papers, and effects." U.S. Const. Amend. IV.

## SUMMARY AND CONCLUSION

In the case at bar, Government law enforcement agents were investigating Defendant for certain computer crimes. Without obtaining a search warrant, presumably because they believed that they did not yet have probable cause (and thus enough information and/or evidence to support the issuance of a search warrant), they attempted to conduct a warrantless search of Defendant's home, and then search,

seize, and then again search his personal computer, during a time period when Defendant was away from home at work. Although Defendant's parents indicated to the Government agents that they consented to some of the law enforcement agents entering the house, to the inspection of their computers, and allowed agents into the rooms in which their computers were situated, an objective review of the circumstances at the time, reveal that their "consent" was probably not voluntary. Even if their consent to allow Government agents to enter the house, and look at their own computers, is deemed voluntary, clearly they did not give agents consent to enter Defendant's computer room, move furniture in order to inspect the laptop computer, open the lid of Defendant's laptop computer, access or run commands on Defendant's laptop computer, or seize the laptop computer. Further, after the computer was in the possession of the FBI agents, but prior to them having obtained a search warrant, law enforcement agents once again accessed and ran commands on Defendant's computer without his consent, or anyone authorized to give consent.

While they were in Defendant's house, there was absolutely nothing, in plain view, which was observed by the law enforcement agents that resulted in them obtaining additional probable cause that Defendant's computer, located in his computer room, was involved in, or was evidence of the computer crimes that they were investigating. As pointed out above, at the time the agents first saw the computer, the laptop lid would have been closed. There would have been no way for them to have seen the computer screen, or viewed any alleged remote access that was taking place. Further, there would have been no way that the screen would have been visible (even assuming arguendo that the laptop lid was slightly open) to someone standing in the

hallway looking into the room, since a chair was directly in front of the computer and would have blocked that person's line of sight. And, if they believed that they had probable cause that that specific computer was involved in the crimes that they were investigating, they certainly would have obtained a search warrant in the first place, before going out to Defendant's house.

With regard to possible exigent circumstances, the law enforcement agents created those very circumstances by going out to Defendant's house without a warrant, and then alerting Defendant as to their investigation of him and his computer. Their unlawful actions in entering Defendant's computer room, and then opening the computer lid and observing the computer screen, caused them to determine that the computer was probably involved in the crimes being investigated. With their improperly obtained observations of the computer screen, coupled with their having given the Defendant knowledge of their investigation, the Government may now seek to use the "exigent circumstances" exception to the warrant requirement. However, Defendant adamantly asserts that this exception is not available to the Government under Kentucky v. King, 563 U.S. 452 (2011), since it was the Government's own unlawful actions, to begin with, that caused the exigent circumstances to arise.

As a result of the observation of Defendant's computer screen, the FBI agents believed that Defendant had remotely accessed his computer from his work computer. Based upon that determination, agents went out to Defendant's employment and seized his work computer. Further, as a result of the subsequent search of Defendant's computer, charges were brought against Defendant, which directly led to him, with counsel, giving two separate proffer statements to the Government – on January 20,

2017 and May 23, 2017. During both of those proffer sessions, Defendant made incriminatory oral statements to the Government investigators. As derivate evidence of an unconstitutional search and seizure, Defendant asserts that those items of evidence should also be subject to the exclusionary rule and suppressed. Further, any and all derivative evidence obtained as a result of Defendant's proffer statements, or derived from computer data found on Defendant's computers must also be suppressed.

Therefore, Defendant respectfully requests that the Court find that Defendant's personal laptop computer, the computer data found on Defendant's personal computer, work computer, and external drives/flash drives, as well as his two proffers statements be suppressed as having been obtained in violation of his Fourth Amendment rights. Any and all other evidence obtained as a result of Defendant's proffer statements, or derivatively obtained from any of the aforementioned computer data must also be suppressed.

Respectfully submitted,

/s/ Thomas E. Conway
Thomas E. Conway (Reg. 0021183)
Attorney for Defendant
55 Public Square Suite 2100
Cleveland, Ohio 44113
(216) 210-0470 - phone
(216) 621-8714 - Fax
teconway@sbcglobal.net - Email

**CERTIFICATE OF SERVICE**

I certify that the forgoing was filed electronically on April 28, 2019. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system, and can be accessed through said system.

/s/ Thomas E. Conway
Thomas E. Conway